AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: /S Bow Bottomly 06/28/2024

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of *(Briefly describe the property to be search* *Or identify the person by name and address)* INSTAGRAM ACCOUNTS WITH USERNAMES fluffy_dragons1089 AND luna_678 USED BY UNKNOWN PERSON(S) THAT ARE STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC.	)	Case No: M-24-536-STE

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following Property *(identify the person or describe property to be searched and give its location)*:

See Attachment A, which is attached and incorporated by reference.

Located in the Northern District of California, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1470	transfer of obscene material to a minor
18 U.S.C. § 2251(a) and (e)	production of child pornography
18 U.S.C. § 2252A	possession and receipt of child pornography

The application is based on these facts:

See attached Affidavit of Special Agent Elizabeth Hancock, Homeland Security Investigations (HSI) , which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of [No. of Days] days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

ELIZABETH HANCOCK
SPECIAL AGENT
HSI

Sworn to before me and signed in my presence.

Date: Jun 28, 2024

Shon T. Erwin

Judge's signature

City and State: Oklahoma City, Oklahoma

SHON T. ERWIN, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Elizabeth Hancock, a Special Agent ("SA") with Homeland Security, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Instagram account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta"), an electronic communications service and/or remote computing service provider headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § § 2703(a), 2703(B)(1)(a) and 2703(c)(1)(A) to require Meta to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been employed as a SA with Homeland Security Investigations ("HSI") since August 2019, and am currently assigned to work human trafficking, child exploitation, and intellectual property rights cases in Oklahoma City, Oklahoma. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. In 2009, prior to becoming a Special Agent, I attended the Police Academy and received a Texas Commission on Law Enforcement ("TCOLE") law enforcement certificate as a Patrol Officer for the Nacogdoches Police Department in

Nacogdoches, Texas. In 2014, I became a Detective at the Angelina County Sheriff's Office in Lufkin, Texas. As a Detective, I predominantly investigated "Crimes Against People," specifically exploitation of children. In securing said commission, I received formal law enforcement training, to include over twenty-three weeks at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia, as it pertains to investigating and enforcing violations of Federal law, including violations of Federal customs and smuggling statutes, as well as child exploitation crimes.

3. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A, (possession and receipt of child pornography), 18 U.S.C. § 2251 (production of child pornography), and 18 U.S.C. § 1470 (transfer of obscene material to a minor) have been committed by the user of the Instagram account with username "te.ll873", and that the evidence of the violations will be found in the Instagram accounts with usernames "te.ll873", "fluffy_dragons1089", and "luna_678". There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C § § 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States…that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or a computer-generated image that is, or is indistinguishable from, the of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such devices: and includes smartphones, and mobile phones and devices." *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other

memory storage devices); peripheral input-output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password, a string of alpha-numeric characters, usually operated what might be termed a digital key to "unlock" data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. "Internet Protocol address," or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigned a user's computer a particular IP address that is used each time the computer accesses the Internet.

g. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web

hosting, email, remote storage, and co-location of computers and other communications equipment.

h. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

i. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

j. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

k. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks; RAM; "thumb," "jump", or "flash" drives; CD/DVDs; and other magnetic or optical media.

l. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on a computer disc or other electronics means which is capable of conversation into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether stored in a permanent format.

PROBABLE CAUSE

7. On May 14, 2024, the HSI Oklahoma City office received a HSI Tip Report regarding an online solicitation of a minor incident that occurred in Oklahoma City, Oklahoma.

The reporter was identified as the child's mother, Erika O'Bar. The child, a 9-year-old female, will be referred to as MV1.

8. In the report, Erika O'Bar stated her daughter reported that an unknown adult male subject sent her explicit images of himself and asked her to send explicit images of herself to him. MV1 sent images of herself but did not tell Erika O'Bar the details of the images. The incident occurred over the messaging and social media platform Instagram, which is owned and operated by Meta.

9. After being notified of the incident, Erika O'Bar made an online report to the National Center for Missing and Exploited Children ("NCMEC"). She also took pictures of the conversation thread and provided those to law enforcement.

10. On June 5, 2024, MV1 was forensically interviewed at the Mary Abbott House, a Children's Advocacy Center located in Normal, Oklahoma. During the interview, MV1 stated an adult male contacted her on Instagram. The username of the suspect's Instagram account was identified as "te.ll873". Username te.ll873 began the conversation by asking MV1 what gender she was, and telling MV1 that he was 12 years old. Username te.ll873 eventually asked MV1 to send images of herself. Username te.ll873 sent MV1 images of his torso to "prove" he was a male. MV1 eventually sent images of herself to user te.ll873, which began with an image of her stomach. Username te.ll873 began telling MV1 to send other pictures of her body parts. Username te.ll873 asked MV1 if he could show MV1 his "boy part". MV1 admitted that she did send te.ll873 images of herself, including her vaginal area and chest area. MV1 stated she used two different accounts to speak to te.ll873 and was not sure which account had the most information on it. One account was identified as luna_678 and the other was identified as fluffy_dragons1089. Both victim

accounts are Instagram accounts and likely under the name "Donna Hurst", which is MV1's grandma and the owner of the phone used by MV1.

11. I was able to corroborate MV1s account of what occurred after reviewing the text part of communications between MV1 and te.ll873 (the child deleted some of her communications). During the course of the communications, te.ll873 told MV1 to send more and more pictures of herself, saying "show more", "No underwear", "is there a hole" and "our secret". Username te.ll873 also asked MV1 to send a video of her whole body. After asking for a video, username te.ll873 sent the messages, "No way u nine" and "Your pussyhole looks so good".

12. Eventually MV1 stopped responding to username te.ll873, so username te.ll873 sent a message stating, "If you don't show more…I will post everything u sent me". Username te.ll873 also sent MV1 an eleven second video of an adult male exposing himself to the camera and fondling himself, including the message, "Do u want to see me cum".

13. On June 5, 2024, a preservation request was sent to Instagram regarding the account with username te.ll873, as well as MV1s accounts with usernames fluffy_dragons1089 and luna_678.

CHARACTERISTICS COMMON TO CHILD PONORGRAPHY COLLECTORS

14. As a result of my consultation with other law enforcement officers, both federal and state, who have considerable experience investigating the sexual exploitation of children, and my own experience, I have learned about the individuals engaged in child exploitation activities and about the computer technology available to, and utilized by, those individuals. I have learned that individuals engaged in the production, procurement, and trade, and/or transmission of child exploitation through the United States mail, computer or other interstate conveyance commonly:

a. Receive sexual gratification and satisfaction from actual physical contact with children and from fantasy that may be simulated by producing and viewing children engaged in sexual activity or in sexually suggestive poses.

b. Own and operate photographic production and reproduction equipment. This equipment is often digital cameras which include both cameras which take still images and movie files.

c. Collect sexually explicit or suggestive materials of adults and/or children consisting of photographs, magazines, motion pictures, videotapes, books, slides, computer images, drawing or other visual media for their own sexual arousal and gratification, and in some instances, or lower the inhibitions of children they are attempting to seduce, and/or to arouse and to demonstrate their desired sexual acts to their selected partners or victims.

d. Often do not dispose of their collection of sexually explicit material. If the material is discarded or lost due to computer malfunction, these individuals often replenish their supply of child exploitation materials very quickly.

e. Correspond with individuals who share their same interest in child exploitation materials, and maintain their names, addresses, telephone numbers, and other identifying information in lists, telephone books, address books, scraps of paper, or on computer disks.

f. Obtain, collect, and maintain photographs of children they are or have been involved with, which may depict children fully clothed, in various stages of undress, totally nude, or in various activities, which are often held for lengthy periods.

g. Collect books, magazines, newspapers, and other writings about sexual assaults of children to understand their own feelings toward children, to justify their feelings, and to find countenance for their illicit behaviors and desires.

h. Commonly collect items which could be any material relating to children that serve a sexual purpose for a given individual. These items as used herein, have been termed "child erotica" and so defined by now retired Special Agent Ken Lanning, Federal Bureau of Investigation. *See* Kenneth Lanning, Child Molesters: A Behavioral Analysis (2001) at page 65. Some of the more common types of "child erotica" include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids. Federal courts have recognized the evidentiary value of child erotica and its admissibility in child exploitation cases. *United States v. Riccardi,* 258 F.Supp.2d 1212 (D. Kan. 2003); *United States v. Caldwell,* 181 F.3d 104 (6th Cir. 1999) (unpublished) (child erotica admissible under Federal Rules of Evidence 404(b) to show knowledge or intent).

i. Often do not discard the child exploitation material but collect it over a long period of time and maintain their material in the privacy of their homes. Sometimes, individuals using peer-to-peer software will engage in a routine where they may delete their child exploitation material after they have viewed it several times and then, after the deletion occurs, the individual will replenish their supply via their peer-to-peer connection when they desire more images to satisfy their sexual interest in children. This procurement and purging cycle results in evidence of their current child exploitation materials being easily located on their computer, as well as evidence of

their deleted material remaining on their computer, which can be recovered by a forensic computer examiner.

j. In my experience and that of other law enforcement agents with experience investigating child exploitation crimes, individuals who trade and share child exploitation material via the Internet retrieve and store the child exploitation materials (whether they produced it or obtained it from other sources) on an electronic storage device as previously stated. As also previously stated, individuals who trade and share child exploitation materials tend to retain their collection of child exploitation materials on digital media (such as hard drives, computer and/or cell phones), which can be stored for a very long amount of time, and tend to keep their collection nearby and secured, usually within their residence or on their person. It is well-known that when individuals relocate from one residence to another, they take their valued possessions (such as vehicles, furniture, clothes, important documents, computer, electronic devices, etc.) with them and store them in their new residence.

k. Based on the facts set forth above, I believe that the person with Instagram username te.ll873 engaged in the above-described illegal activities and that a search of their Instagram account, along with Instagram accounts with usernames "fluffy_dragons1089" and "luna_678" will result in the evidence related to the offenses of production, receipt and possession of child pornography material.

COMPUTERS, THE INTERNET, AND CHILD EXPLOITATION

15. I have had training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child exploitation interact with each other. Computers basically serve four functions in connection with child exploitation: production, communication, distribution, and storage.

b. Individuals involved in child exploitation can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 256 gigabytes of data, which provides enough space to store thousands of high-resolution photographs and videos. Video camcorders, which once recorded video onto tape or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Electronic contact can be made to millions of computers around the world. The ability to produce child exploitation images/videos easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child exploitation images/videos. Child exploitation can

be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child exploitation materials.

d. The Internet affords individuals several different venues for obtaining, viewing, and trading child exploitation materials in a relatively secure and anonymous fashion. For example, distributors of child exploitation materials can use membership-based/subscription-based Web sites to conduct business, allowing them to remain relatively anonymous.

e. Individuals also use online resources to retrieve and store child exploitation materials, including services offered by Internet Portals such as Yahoo! and Instagram, among others. The online services allow a user to set up an account with a remote computer service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases here online storage is used, however, evidence of child exploitation can be found on the user's computer or external media in most cases.

BACKGROUND CONCERNING INSTAGRAM[1]

16. Instagram is a service owned by Meta Platforms, a United States company and provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510.

[1] The information in this section is based on information published by Facebook on its website and its Instagram website, including, but not limited to, the following webpages: "Data Policy," https://help.instagram.com/519522125107875; "Information for Law Enforcement," https://help.instagram.com/494561080557017; and "Help Center," https://help.instagram.com.

Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

17. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

18. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the IP addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

19. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account or transfer an image from Instagram to a connected image printing service. Facebook maintains

records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Facebook and third-party websites and mobile apps.

20. Instagram users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also "block" other users from viewing their posts and searching for their account, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments. Instagram also allows users to create a "close friends list" for targeting certain communications and activities to a subset of followers.

21. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Facebook to access the contact lists on their devices to identify which contacts are Instagram users. Facebook retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Facebook to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

22. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

23. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can

remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Facebook's servers.

24. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

25. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Facebook's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

26. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

27. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the

recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

28. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

29. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Facebook retains records of a user's search history and followed hashtags.

30. Facebook collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Facebook to personalize and target advertisements.

31. Facebook uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Facebook maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

32. In some cases, Instagram users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from

other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

33. For each Instagram user, Facebook collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

34. In my training and experience, suspects will utilize social media platforms such as Instagram and other photo and video sharing sites to perpetrate crimes, including crimes against children. It is believed the named account(s) will yield evidence showing criminal activities, including production, receipt, and possession of child sexual exploitation materials possibly being shared through the Instagram platform or other social media and peer-to-peer sites. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

35. It is believed further evidentiary information will be found in the stored communications of the accounts, including possible other accounts. For example, the stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails,

voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

36. The identity of the individuals utilizing these account(s) is pertinent to further investigative avenues by the Agency. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

37. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

38. Other information connected to the use of Instagram may lead to the discovery of additional evidence. For example, the accounts mentioned may be in communication with other victims or suspects. Emails, instant messages, Internet activity, documents, and contact and

calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

39. Reviewing the communication threads and bodies of messages in the account(s) are likely to contain information and evidence related to the crimes mentioned, possession, receipt, and production of child pornography. Therefore, Instagram's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

40. Based on the foregoing, I request that this Court issue the proposed search warrant. Because the warrant will be served to Meta, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Elizabeth Hancock
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on the 28th day of June, 2024

SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

41. This warrant applies to information associated with the Instagram account "fluffy_dragons1089", and "luna_678" active on, but not limited to January 1, 2024 through June 20, 2024, that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc, a company that accepts service of legal process at 1 Meta Way, Menlo Park, California 94025.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. ("Meta"):

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is stored, held, or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A:

A. All business records and subscriber information, in any form kept, pertaining to the account, including:

1) Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;

2) All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);

3) Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;

4) Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;

5) All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6) Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, from January 1, 2024, to June 20, 2024;

7) Privacy and account settings, including change history; and

8) Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;

B. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from January 1, 2024, to June 20, 2024;

C. All content, records, and other information relating to communications sent from or received by the account from January 1, 2024, to June 20, 2024, including but not limited to:

1) The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;

2) All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);

3) All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and

4) All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the account and other Instagram users from January 1, 2024, to June 20, 2024, including but not limited to:

1) Interactions by other Instagram users with the account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2) All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3) All contacts and related sync information; and

4) All associated logs and metadata;

E. All records of searches performed by the account from January 1, 2024, to June 20, 2024; and

F. All location information, including location history, login activity, information geotags, and related metadata from January 1, 2024, to June 20, 2024.

II. Information to be seized by the government:

All information described above in Section I that constitutes fruits, contraband, evidence and/or instrumentalities of violations of 18 U.S.C. §§§ 1470, 2251 and 2252A from January 1, 2024, though June 20, 2024, including for each user account or identifier listed on Attachment A, information pertaining to the following matters:

a. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner.

b. Evidence indicating the account owner's state of mind as it relates to the crime under investigation.

c. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

d. Evidence related to communications involving the users of the account with username te.ll873 concerning the above discussed offenses.

e. Evidence related to communications involving the users of the account with username te.ll873 and the users of Instagram account with usernames fluffy_dragons1089 and luna_678.

f. Evidence related to communications involving the users of the account with username te.ll873 and any minors using Instagram accounts regarding other violations of 18 U.S.C. §§§ 1470, 2251 and 2252A.

g. Evidence related to the production, possession, and receipt of child exploitation as defined in 18 U.S.C. § 2256(8).

h. Evidence concerning minors visually depicted while engaging in sexually explicit conduct as defined in 18 U.S.C. §2256(2).

i. Names, addresses, and/or other contact information of individuals who may have been contacted by individual(s) concerning the production, possession, receipt, or distribution of child exploitation as defined in 18 U.S.C. §2256(8), including records that help reveal their whereabouts.

j. All the non-content records describe above in Section I.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Meta Platforms, Inc. ("Meta"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Meta. The attached records consist of

_____

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Meta, and they were made by Meta as a regular practice; and

b. such records were generated by Meta's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Meta in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Meta, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature